

FIG. 1

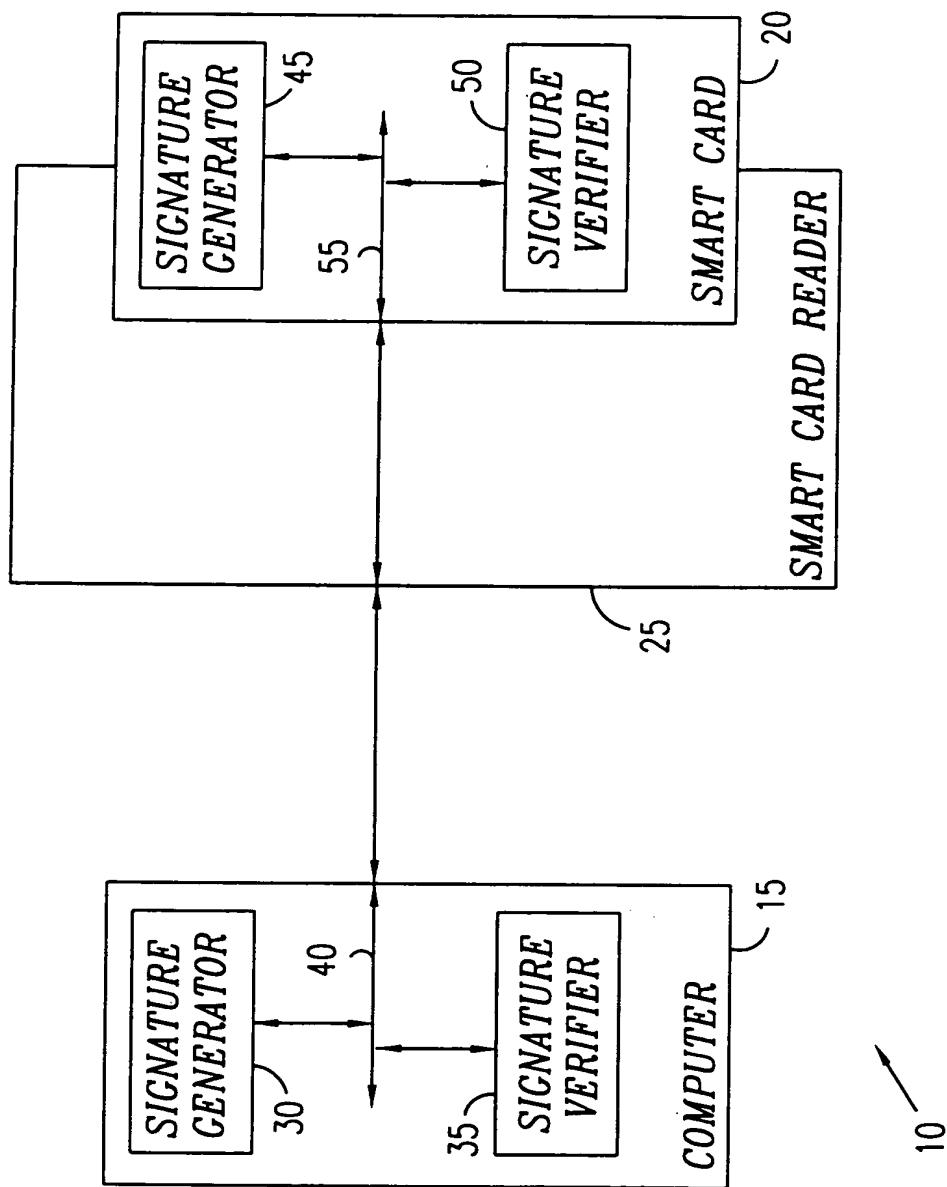


FIG. 2A

A GENERATOR OF A PUBLIC-KEY SUPPLIES A SET S1 OF k POLYNOMIAL FUNCTIONS AS A PUBLIC-KEY, WHERE THE SET S1 INCLUDES THE FUNCTIONS

$P_1(x_1, \dots, x_{n+v}, y_1, \dots, y_k), \dots, P_k(x_1, \dots, x_{n+v}, y_1, \dots, y_k)$, WITH k, v, AND n BEING INTEGERS, x_1, \dots, x_{n+v} BEING n+v VARIABLES OF A FIRST TYPE, AND y_1, \dots, y_k BEING k VARIABLES OF A SECOND TYPE, AND THE SET S1 BEING OBTAINED BY APPLYING A SECRET KEY OPERATION ON A SET S2 OF k POLYNOMIAL FUNCTIONS

$P'_1(a_1, \dots, a_{n+v}, y_1, \dots, y_k), \dots, P'_k(a_1, \dots, a_{n+v}, y_1, \dots, y_k)$ WITH a_1, \dots, a_{n+v} BEING n+v VARIABLES WHICH INCLUDE A SET OF n "OIL" VARIABLES a_1, \dots, a_n , AND A SET OF v "VINEGAR" VARIABLES a_{n+1}, \dots, a_{n+v}

A MESSAGE TO BE SIGNED IS PROVIDED

A SIGNER OF A DIGITAL SIGNATURE APPLIES A HASH FUNCTION ON THE MESSAGE TO PRODUCE A SERIES OF k VALUES b_1, \dots, b_k

THE SIGNER SUBSTITUTES THE SERIES OF k VALUES b_1, \dots, b_k FOR THE VARIABLES y_1, \dots, y_k OF THE SET S2 RESPECTIVELY SO AS TO PRODUCE A SET S3 OF k POLYNOMIAL FUNCTIONS $P''_1(a_1, \dots, a_{n+v}), \dots, P''_k(a_1, \dots, a_{n+v})$

THE SIGNER SELECTS v VALUES $a'_{n+1}, \dots, a'_{n+v}$ FOR THE v "VINEGAR" VARIABLES a_{n+1}, \dots, a_{n+v}

THE SIGNER SOLVES A SET OF EQUATIONS $P''_1(a_1, \dots, a_n, a'_{n+1}, \dots, a'_{n+v})=0, \dots, P''_k(a_1, \dots, a_n, a'_{n+1}, \dots, a'_{n+v})=0$ TO OBTAIN A SOLUTION FOR a'_1, \dots, a'_{n+v}

THE SIGNER APPLIES THE SECRET KEY OPERATION TO TRANSFORM a'_1, \dots, a'_{n+v} TO THE DIGITAL SIGNATURE e_1, \dots, e_{n+v}

FIG. 2B